

# Very Low Cost Entropy Source Based on Chaotic Dynamics Retrofittable on Networked Devices to Prevent RNG Attacks

Mattia Fabbri  
University of Bologna, Italy  
mattia.fabbri2@studio.unibo.it

Sergio Callegari  
ARCES/DEI, University of Bologna, Italy  
sergio.callegari@unibo.it

**Abstract**—Good quality entropy sources are indispensable in most modern cryptographic protocols. Unfortunately, many currently deployed networked devices do not include them and may be vulnerable to Random Number Generator (RNG) attacks. Since most of these systems allow firmware upgrades and have serial communication facilities, the potential for retrofitting them with secure hardware-based entropy sources exists. To this aim, very low-cost, robust, easy to deploy solutions are required. Here, a retrofittable, sub 10\$ entropy source based on chaotic dynamics is illustrated, capable of a 32 kbit/s rate or more and offering multiple serial communication options including USB, I<sup>2</sup>C, SPI or USART. Operation is based on a loop built around the Analog to Digital Converter (ADC) hosted on a standard microcontroller.

## I. INTRODUCTION

One of the most powerful trends recently seen in technology is the networking of a large number of devices originally operating in isolation. By 2020 more than 25 billion devices will be interconnected [1]. This Internet of Things (IoT) can bring smartness to many environments whose items gain the ability to cooperate and a richer set of information to base their behaviors upon. At the same time, making a huge number of devices remotely reachable poses profound security challenges because of the immense attack surface [2].

Unfortunately, many devices being brought online lack certain security-oriented subsystems. This is due to cost and conception, since networking is often applied to mundane items and awareness on security issues is still growing. In a short time, there will be a huge legacy of networked devices missing hardware parts critical to security. This can be long lasting since humble devices lack any upgrade lust and are only substituted when they break, as users often fail to see potential threats as lack of functionality. Surveys reveal that about half of the networked devices found in businesses are already on the brink of obsolescence [3]. To contrast this phenomena, some authors suggest that embedded networking units should be given a scheduled end-of-life [4]. Until this is a reality (if ever), the alternative is to minimize the costs of patching current devices, either in manufacturing, through design revisions, or on field, through software upgrades and hardware retrofits.

This paper illustrates the design of a hardware primitive critical for security, namely an entropy source, whose absence can favor Random Number Generator (RNG) attacks (references to past incidents in [5]). True-RNGs and hardware entropy sources are becoming mainstream in computers [6], but are still missing from most low-cost/embedded

This is a post-print version of a paper published in the Proceedings of 2014 IEEE International Conference on Electronics, Circuits, and Systems (ICECS). Cite as:

Fabbri M., Callegari S., “Very Low Cost Entropy Source Based on Chaotic Dynamics Retrofittable on Networked Devices to Prevent RNG Attacks,” *IEEE 21th International Conference on Electronics, Circuits, and Systems (ICECS 2014)*, pp. 175–178, Dec. 2014.

Copyright [Pleaseinsert\PrerenderUnicode{\hat{A}}] 2014 IEEE. Personal use of this material is permitted. However, permission to use this material for any other purposes must be obtained from the IEEE by sending a request to [pubs-permissions@ieee.org](mailto:pubs-permissions@ieee.org).

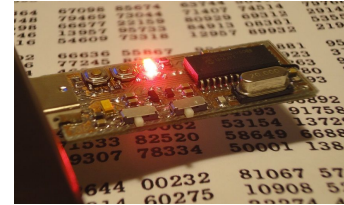


Figure 1. Prototype of self-contained entropy source with USB port, including diagnostic LEDs, control switches, trimmers, test-pads, and a DIP  $\mu$ C package significantly enlarging the layout.

devices. The current proposal can be declined in multiple forms: from a self-contained plug-in applicable on field to existing systems (Fig. 1) to a schematic upgrade re-using an existent microcontroller ( $\mu$ C), targeting manufacturers. In either case, key features are: (i) very low cost (sub-10\$ for a self-contained unit with Universal Serial Bus (USB) connector, sub-5\$ for designs where a  $\mu$ C is available to share); and (ii) high interconnection flexibility (USB, I<sup>2</sup>C, SPI or USART interfaces, depending on the adopted  $\mu$ C) in order to favor adoption as a retrofit. The entropy rate that can be delivered is in the few tens kbit/s range, depending on the  $\mu$ C (over 32 kbit/s have been experimentally observed with a PIC18F2550).

Similar solutions are scarce on the market, with true-RNG retrofits ranging from near 40\$ to over 1000\$ (i.e., at far higher costs, even considering selling margins). Closest competitors are the TRNG98 modules [7], and the Simtec Entropy Key. Differently from any other design, the current proposal is based on chaotic dynamics, rather than direct amplification of electronic noise (thermal, avalanche, etc.), which can make the system less susceptible to tampering and side channel attacks [8]. It is not the first time that chaos is proposed for RNGs [9], but the current design has the distinguished feature of re-using Analog to Digital Converters (ADCs) readily available on  $\mu$ Cs. ADC reuse, originally introduced in [10], has already seen experimental validation [8], but so far only on full-custom integrated circuits with ad-hoc designed *pipeline* ADCs, where stages can be separated from each other. Here, taking advantage of the generalized theory in [11], [12], the approach is used for the first time on an unmodified commercial ADC, with a successive approximation architecture and harsh operating conditions ( $\mu$ C ADCs are often poorly isolated from digital noise). This setup requires some specific design arrangements that are here thoroughly detailed.

## II. BACKGROUND: RNGS AND SECURITY

Cryptographic systems base their operation on the existence of some secret data known to authorized users and unpredictable by others. To warrant unpredictability, random strings are often employed, e.g., in *keys*, *salts*, *nonces*, *initialization vectors*, *challenges*, and other one-time quantities. Generating these strings can be non-trivial, since digital system, by nature, cannot behave randomly. Compromises

have traditionally been made, using algorithms, known as pseudo-RNGs, capable of expanding short *seeds* into irregular long sequences. Unfortunately, this has recently lead to security incidents. In fact, discovery of the algorithm state by an attacker provides the ability to predict future ‘random’ quantities [13]. In some cases, RNG attacks had a high impact, pushing big players of information technology to incorporate true-RNGs in their larger and newer systems [6].

For simpler or legacy systems, software solutions have been developed capable of gathering noisy data (entropy) from peripherals ‘perceiving’ physical phenomena complex enough to be assumed random. For instance, many operating systems have access to mouse movements, key press timings, hard disk latencies, etc. Such quantities are irregular, but may show correlations. Yet, they can be accumulated in buffers from which good random numbers can be *distilled* through operations such as *hashing* and the frequent *re-seeding* of pseudo-RNGs [14]. This works fairly well for standard computers, but may fail for little devices in an IoT scenario. In fact, the latter may lack most of the peripherals needed to collect entropy (for instance, little routers, networked thermostats, and so on do not have mice, keyboards or hard-disks). With this, attempts at entropy distillation may even become counterproductive, giving a false sense of security while in fact falling back to pseudo-RNG behavior due to lack of inputs.

The ultimate fix is clearly to bring true-RNGs even to humble devices. Doing so in the form of hardware retrofits needs carefully weighing the available options. Ultimately, true-RNGs are *analog* systems that harvest information from physical phenomena so intricate at the microcosmic level to appear random at the macroscopic scale. Their simplest implementation consists in the direct amplification and acquisition of electronic noise (thermal, avalanche, etc). This can be effective but is inherently exposed to tampering, since interference may be easily exchanged from genuine noise, so that (expensive) shields can be mandatory [7]. Another form of amplification is to exploit the meta-stability of positive feedback structures. A further alternative is to deploy phase noise in oscillators that mutually sample each other. This lets the analog quantity be *time*, so that digital voltage levels can be adopted. Furthermore, susceptibility to tampering is improved by the more indirect harvesting. Finally, at the highest level of sophistication, one finds circuits based on chaotic dynamics.

The chaos-based approach is inherently different from all the others. First of all, chaotic-RNGs replicate at the circuit level some of the features, including *sensitivity to initial conditions* [15], conjectured to be at the root of randomness in natural systems. Secondly, they harvest noise in a radically different way. Non-chaotic sources need to continuously gather new noise samples, while chaotic source could in principle use just the uncertainty in their start-up condition, thanks to sensitivity to initial conditions. In practice, noise will certainly be present throughout all the operating time, but this ends up being just a bonus, since correct functionality does not strictly demand it. For this reason, as long as it is independent from their inner state, noise or interference collected *during* operation can often bear only minor influence on output quality (unless it is very large, but in this case tampering can typically be detected with ease).

### III. ADC BASED TRUE-RNG

Among all possible chaotic sources, discrete time ones based on the iteration of 1-dimensional Piece-Wise Affine Markov (PWAM) maps [10] are very appealing. The corresponding model is

$$x(n+1) = M(x(n)) \quad (1)$$

where an invariant set (here normalized to  $[0, 1]$ ) exists for  $M(\cdot)$ . The PWAM nature of  $M(\cdot)$  assures that a partition  $\mathcal{P}$  of  $[0, 1]$  exists such that the dynamics, once observed through a  $\mathcal{P}$ -induced quantization function  $q(x)$ , can be modeled through a Markov chain [11].

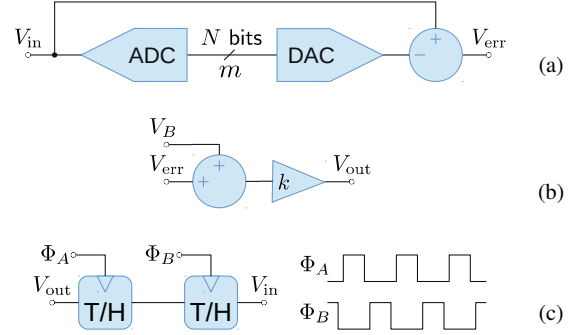


Figure 2. Derivation of ADC quantization error via a cascaded DAC (a); its processing (b); and the closing of the loop to create a chaotic with a shift-type map (c).

Shift type maps, such as

$$M(x) = (\alpha x + \beta) \bmod 1 \quad (2)$$

with integer  $\alpha > 1$  are particularly interesting. They assure that any subdivision of  $[0, 1]$  in  $\alpha$  equally sized sub-intervals, wrapped around at the invariant set boundaries, results in a Markov partition regardless of  $\beta$ . Namely, the partition can be built taking any  $p \in [0, 1]$  and sets  $I_i$  for  $i = 0, \dots, \alpha - 1$ , such that

$$I_i = \{x : x \in [0, 1] \wedge i \leq \alpha((x - p) \bmod 1) < i + 1\} . \quad (3)$$

The corresponding Markov chain has  $\alpha$  states, with transition probabilities among any two of them equal to  $1/\alpha$ . In other words, it is identical to the chain describing the cast of an  $\alpha$ -faced unbiased die [11]. Thus, the system has the ability to generate random symbols.

Interestingly, shift maps can be easily obtained by deriving the quantization error of an ADC, as shown in Fig. 2(a). Let  $ADC(V)$  and  $DAC(m)$  be used to indicate the static characteristics of the ADC and the Digital to Analog Converter (DAC), respectively. For an  $N$  bit single ended ADC, one should ideally have

$$ADC(V) = \left\lfloor \frac{2^N}{V_{ref}} V \right\rfloor \quad (4)$$

where  $V_{ref}$  is the reference voltage (approximately equal to the full scale) and a *flooring* ADC behavior is assumed. Quantization step is  $V_{ref}/2^N$ . For the complementary  $N$  bit DAC one has

$$DAC(m) = m \frac{V_{ref}}{2^N} \quad (5)$$

so that the quantization error, estimated as show in the figure is

$$\begin{aligned} V_{err} &= V_{in} - DAC(ADC(V_{in})) = V_{in} - \frac{V_{ref}}{2^N} \left\lfloor \frac{2^N}{V_{ref}} V_{in} \right\rfloor = \\ &= \frac{V_{ref}}{2^N} \left( \frac{2^N}{V_{ref}} V_{in} - \left\lfloor \frac{2^N}{V_{ref}} V_{in} \right\rfloor \right) = \frac{V_{ref}}{2^N} \left( \frac{2^N}{V_{ref}} V_{in} \bmod 1 \right) . \end{aligned} \quad (6)$$

The expression already contains the modulus operation that characterizes Eqn. (2). Now, assume that a further block, as shown in Fig. 2(b) computes  $V_{out} = k(V_{err} + V_B)$ . Altogether

$$V_{out} = \frac{k V_{ref}}{2^N} \left( \frac{2^N}{V_{ref}} V_{in} \bmod 1 \right) + k V_B . \quad (7)$$

Rearranging the terms, one has

$$\begin{aligned} \frac{2^N}{k V_{ref}} (V_{out} - k V_B) &= \\ &= \left( k \frac{2^N}{k V_{ref}} (V_{in} - k V_B) + k \frac{2^N}{V_{ref}} V_B \right) \bmod 1 . \end{aligned} \quad (8)$$

It is now sufficient to introduce the voltage-to- $x$  transformation

$$x \rightarrow \frac{2^N}{kV_{\text{ref}}}(V - kV_B) \quad V \rightarrow \frac{kV_{\text{ref}}}{2^N}x + kV_B \quad (9)$$

to see that Eqn. (8) defines the map  $M(\cdot)$ , with  $\alpha \equiv k$  and  $\beta \equiv k2^N V_B/V_{\text{ref}}$ . From this, to obtain a dynamical system such as that in Eqn. (1), it is enough to feed back  $V_{\text{out}}$  into  $V_{\text{in}}$  through a delay element. The latter can be implemented as the cascade of two Track-and-Holds (T/Hs) blocks operating in a master-slave fashion, as in Fig. 2(c). With this, while  $x$  spans  $[0, 1]$ , the voltages  $V_{\text{in}}$  and  $V_{\text{out}}$  span  $[kV_B, k(V_B + V_{\text{ref}}/2^N)]$ . The situation is illustrated in Fig. 3, from which it is evident that some bounds are needed for the parameters. Specifically,  $2 \leq k \leq 2^N$  (with  $k \in \mathbb{N}$ ),  $V_B \geq 0$  and  $k(V_B + V_{\text{ref}}/2^N) \leq V_{\text{ref}}$ , i.e.,  $V_B \leq V_{\text{ref}}/k - V_{\text{ref}}/2^N$ .

Interestingly, the figure also makes evident that the ADC quantization inherently provides a  $k$ -state Markov partition for the map. In fact, the range  $[kV_B, k(V_B + V_{\text{ref}}/2^N)]$  is as wide as  $kV_{\text{ref}}/2^N$ , and contains exactly  $k$  quantization steps. Specifically, it is sufficient to take  $p = (m_{\text{min}} + 1)V_{\text{ref}}/2^N$  in order to have  $k$  intervals such as those in Eqn. (3). This is convenient, since it lets the Markov state be directly readable from the output  $m$  of the ADC. In detail, one gets that the spanned  $m$  values fit between

$$m_{\text{min}} = \left\lfloor \frac{2^N}{V_{\text{ref}}} kV_B \right\rfloor \quad m_{\text{max}} = \left\lfloor \frac{2^N}{V_{\text{ref}}} kV_B + k \right\rfloor \quad (10)$$

and that system is in state  $I_i$  when

$$\begin{cases} m = m_{\text{min}} + i + 1 & \text{if } i < k - 1 \\ m = m_{\text{min}} \vee m = m_{\text{max}} & \text{if } i = k - 1 \end{cases} \quad (11)$$

With this, one has a true-RNG that randomly picks a value in an alphabet of  $k$  symbols at each cycle. As an example, Fig. 4 shows the Markov chain corresponding to the setup in Fig. 3. In view of an efficient implementation, it is clearly convenient to make  $k$  a power of 2, say  $2^M$  with  $M \in \mathbb{N}$ , so that each generated value fits exactly in  $M$  bits. Clearly, one needs  $M \leq N$ . In principle,  $M$  should be large so that many random bits can be generated per cycle. Yet,  $M$  and  $N$  must often be contained to ease implementation.

#### IV. PRACTICAL IMPLEMENTATION ON A $\mu\text{C}$

##### A. Implementation principles

Intuitively, the concepts illustrated so far can be easily materialized by a  $\mu\text{C}$  based architecture as shown in Fig. 5. Since most  $\mu\text{Cs}$  already include an ADC, the number of external components can be very low. The loop corresponding to the model in Eqn. (1) can be closed via an external DAC (for instance, the MPC4901 or MPC4911, communicating with the  $\mu\text{C}$  on the SPI bus). The loop gain and offset

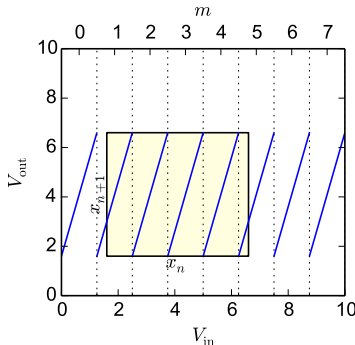


Figure 3. Sample map obtained from the quantization error of an ADC. Here,  $N = 3$ ,  $k = 4$ ,  $V_{\text{ref}} = 10 \text{ V}$ ,  $V_B = 0.4 \text{ V}$ .

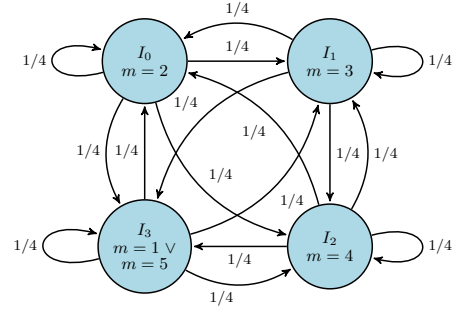


Figure 4. Markov chain corresponding to the map in Fig. 3.

can be provided by a difference amplifier (for instance, obtained by half an LVM602 or LMV792 chip), controlling  $k$  and  $V_B$  by means of its resistors ( $R_A$  to  $R_F$  in the schematic). The loop delay requires two T/H units. These can be obtained by Operational Amplifiers (OAs) with an output enable feature, followed by suitably large capacitors (for instance each T/H can be obtained by an LVM601). A voltage reference is required for accurate operation. Some  $\mu\text{Cs}$  readily provide one, otherwise a dedicated chip (such as the MAX6004) can be used. In the proposed architecture, the loop path goes through the  $\mu\text{C}$ , which acquires the T/H output and passes the corresponding numerical data to the external DAC via its SPI bus. The  $\mu\text{C}$  is also in charge of generating the timing signals for the DAC and the T/H units. These are transferred via 3 lines on one of the digital I/O ports. For prototyping a stand alone unit, the PIC18F2550  $\mu\text{C}$  can conveniently be selected, in view of its low price and integrated USB bus, which favors interfacing. In fact, many little network devices include USB connection facilities. Alternatively, the portion of schematic in Fig. 5(b) can be added to an existing design including a  $\mu\text{C}$  with some spare computational resources. With this, costs can be further lowered.

A notable advantage of the proposal is that it makes  $m$  readily available inside the  $\mu\text{C}$ . Consequently, at each cycle, the  $\mu\text{C}$  can compute a random symbol from it while passing it to the DAC. The so generated symbols can be progressively accumulated and packed in bytes. When the  $\mu\text{C}$  has buffered enough of them (or when a request

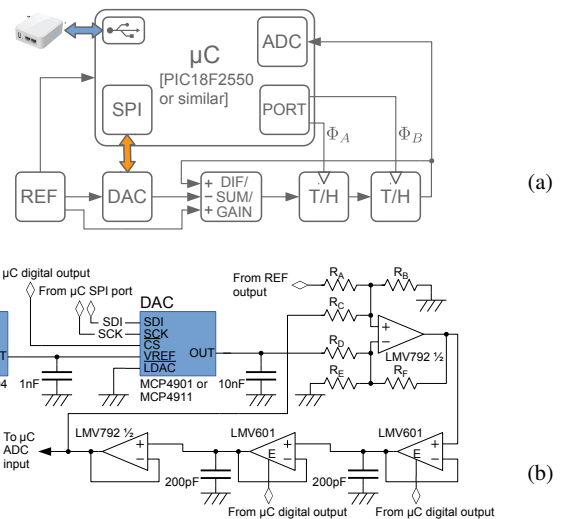


Figure 5.  $\mu\text{C}$  based architecture implementing the proposed true-RNG. Block diagram (a) and signal processing chain added to the  $\mu\text{C}$  (b).

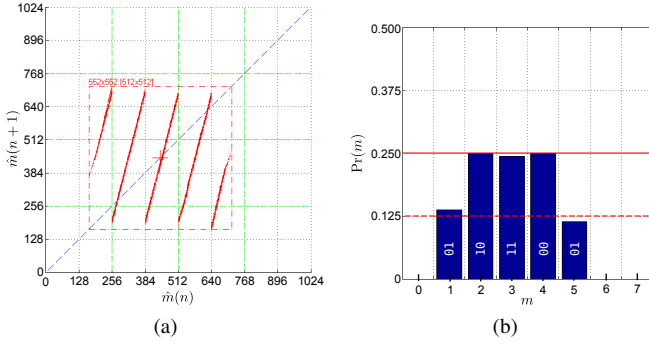


Figure 6. Experimental evaluation of the system prototype illustrated in Fig. 1, set up for  $\hat{N} = 10$ ,  $N = 3$ ,  $M = 2$ ,  $V_{\text{ref}} = 4.096$  V,  $V_B = 192$  mV. Left: shape of the implemented  $M(x)$ , reconstructed by plotting  $\hat{m}(n+1)$  vs  $\hat{m}(n)$ . Right: statistical distribution of  $m$ .

arrives), they can be transferred to the embedding system via one of the  $\mu\text{C}$  communication interfaces, for instance, the USB bus, possibly under encryption to prevent snooping or tampering.

### B. Implementation requirements

In practice, the implementation cannot be so direct and requires some care. Specifically, it is not possible to straightforwardly deploy the block diagram in Fig. 2, because of implementation uncertainties. For instance, in most  $\mu\text{C}$ , the ADC least significant bits (lsbs) can be quite erratic due to couplings with digital lines. Furthermore, accuracy in the setting of  $V_B$  should be in the order of half a quantization step, but this is too fine to achieve when the ADC resolution is 8–10 bits. Any implementation attempt ignoring these matters would most certainly fail. Fortunately, the two issues can be easily worked around by artificially degrading the ADC resolution before computing  $V_{\text{err}}$ . This can be done as follows. Assume that  $\hat{N}$  is the nominal ADC resolution and that  $\hat{m}$  is the actual  $\hat{N}$ -bit ADC output at each cycle, then let  $N$  be just a portion of  $\hat{N}$ , so that  $m$  can be obtained by shifting  $\hat{m}$  right by  $\hat{N} - N$  bits. With this, the value to be passed to the DAC can be obtained by back shifting  $m$  to the left with zero padding. Incidentally, this permits the use of an external DACs with a lower resolution  $\tilde{N} < \hat{N}$ , as long as  $\tilde{N} \geq N$ . Good  $N$  values can be 3 to 5 bits. Furthermore,  $M$  (which determines  $k = 2^M$ ) must be taken to be strictly less than  $N$ . In fact, this lets  $V_B$  be chosen so that the  $V_{\text{out}}$  range lies with clearance within the ADC input range and the OA output saturation voltages. Good  $M$  values are 2 to 4 bits, depending on  $N$ , while good  $V_B$  values let  $kV_B$  fall halfway between voltages corresponding to transition points for  $m$ .

An advantageous side effect of the artificial resolution degradation is that it lets the  $\mu\text{C}$  observe the chaotic system state  $x$  via  $\hat{m}$ , i.e., at a resolution  $\hat{N}$  higher than the  $N$  bits required for operation. In other words, one gains insight on the *analog* system state without the need for external instrumentation. Such an opportunity can be useful in view of self diagnostics or automatic detection of tampering attempts. As an example, Fig. 6(a) shows a reconstruction of the iterated map obtained by *actual experimental data* acquired by the  $\mu\text{C}$  itself.

### C. Experimental validation

The proposed architecture has been extensively tested, using the prototype illustrated in Fig. 1. For the tests, parameters have been set as in the caption of Fig. 6. Pane (b) shows the experimentally obtained  $m$  values and their relative frequencies. The numbers on the graph columns indicate the output bits associated to each  $m$  value (obtained as  $m \bmod 4$ ). Their occurrence probability is well balanced at approximately  $1/4$ . Long output streams have been tested

for their information content, achieving  $> 0.99$  bits of entropy for each delivered output bit (estimated via a marginal entropy approach). The NIST 800-22 suite [16] has also been applied. The corresponding tables of outcomes cannot fit in this paper, but are worth summarizing. The raw generator is incapable of passing *all* tests (though it can already pass many of them). Yet, a minimal post-processing (by a Von Neumann corrector or the XORing of consecutive bits) is already sufficient for full conformance. Similarly, when the raw data produced by the generator is used to feed the entropy distiller in the Linux Operating System (OS), the distiller output can pass all tests.

## V. CONCLUSIONS

A new architecture of a  $\mu\text{C}$  based true-RNG has been proposed, prototyped and tested. Internally it relies on chaotic dynamics. Expected cost is extremely low and many interconnection options are possible, making it suitable as a retrofit for existing networked units that lack a true-RNG and that may be exposed to RNG attacks.

## REFERENCES

- [1] P. Middleton, P. Kjeldsen, and J. Tully, “Forecast: The internet of things, worldwide, 2013,” Gartner, Report G00259115, Nov. 2013.
- [2] R. Roman, P. Najera, and J. Lopez, “Securing the internet of things,” *IEEE Computer*, vol. 44, no. 9, p. 51–58, 2011.
- [3] S. Lynn, “Survey: Biz network devices vulnerable, almost obsolete,” *PC Magazine (Online)*, May 2011. [Online]. Available: <http://www.pcmag.com/article2/0,2817,2385833,00.asp>
- [4] D. Geer, “Security of things,” presented at the Security of Things Forum, Cambridge, MA, USA, May 2014, keynote speech. [Online]. Available: <http://geer.tinho.net/geer.secot.7v14.txt>
- [5] Wikipedia, “Random number generator attack,” 2014, accessed 2014-05-13. [Online]. Available: [http://en.wikipedia.org/wiki/Random\\_number\\_generator\\_attack](http://en.wikipedia.org/wiki/Random_number_generator_attack)
- [6] G. Taylor and G. Cox, “Digital randomness,” *IEEE Spectr.*, vol. 48, no. 9, p. 32–58, 2011.
- [7] B. D. Electronics, “TRNG9880 random number processing,” Dec. 2013, white paper. [Online]. Available: [www.trng98.se/getfile.php?file=trng9880\\_info.pdf](http://www.trng98.se/getfile.php?file=trng9880_info.pdf)
- [8] F. Pareschi, G. Scotti, L. Giancane, R. Rovatti, G. Setti, and A. Trifiletti, “Power analysis of a chaos-based random number generator for cryptographic security,” in *Proc. IEEE Intern. Symp. on Circuits and Systems*, 2009, 2009, pp. 2858–2861.
- [9] S. Callegari, R. Rovatti, and G. Setti, “First direct implementation of true random source on programmable hardware,” *International Journal of Circuit Theory and Applications*, John Wiley & Sons, vol. 33, no. 1, pp. 1–16, 2005. DOI:10.1002/cta.301
- [10] S. Callegari, R. Rovatti, and G. Setti, “Embeddable ADC-based true random number generator for cryptographic applications exploiting nonlinear signal processing and chaos,” *IEEE Trans. Signal Process.*, vol. 53, no. 2, pp. 793–805, Feb. 2005. DOI:10.1109/TSP.2004.839924
- [11] S. Callegari and G. Setti, “ADCs, chaos and TRNGs: a generalized view exploiting Markov chain lumpability properties,” in *Proc. of ISCAS*, New Orleans, LA (USA), May 2007, pp. 213–216. DOI:10.1109/ISCAS.2007.378314
- [12] S. Callegari, “Introducing *Complex Oscillation Based Test*: an application example targeting analog to digital converters,” in *Proc. of ISCAS*, Seattle, WA (USA), May 2008, pp. 320–323. DOI:10.1109/ISCAS.2008.4541419
- [13] D. E. Eastlake, J. I. Shiller, and S. D. Crocker, “Randomness requirements for security,” RFC 4086, Internet Engineering Task Force, 2005. [Online]. Available: <http://www.ietf.org/rfc/rfc4086.txt>
- [14] Z. Gutterman, B. Pinkas, and T. Reinman, “Analysis of the linux random number generator,” in *Proc. of the IEEE Symposium on Security and Privacy*, Oakland, CA, USA, May 2006.
- [15] E. Ott, *Chaos in dynamical systems*. Cambridge University Press, 1993.
- [16] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, National Institute for Standards and Technology Special publication 800-22, May 2001. [Online]. Available: <http://csrc.nist.gov/rnd/SP800-22b.pdf>